UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/895,801	06/29/2001	Larry Brown	41992-00427	5589

7590 10/21/2005

MARSH FISCHMANN & BREYFOGLE LLP
3151 South Vaughn Way, Suite 411
Aurora, CO 80014

EXAMINER	
ABYANEH, ALI S	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/895,801	BROWN ET AL.	
	Examiner	Art Unit	
	Ali S. Abyaneh	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 are presented for examination.

2. Examiner withdraws objection to the abstract due to correction by the applicant.

Response to Arguments

3. Applicant's arguments filed 07-01-2005 have been fully considered but they are not persuasive.

Regarding claims 1-12

Applicant argues that Fahlman **does not receive a message from a first system and transmit it to the to a second system after sanitization.** Examiner respectfully disagrees. Fahlman clearly discloses any of the steps 201 through 207 in fig 2 could be perform at several different location, in another word message generated in step 201 could be in a location different than where it is sanitized (step 205)(see column 4, lines 60-62, fig 2,item 205-209 and fig 6 item 301 and 303), therefore message could be sent for sanitization from any location including from the first system. Secondly even if Fahlman would not teach receiving a message from a first system and transmitting it to a second system still applicant's argument would not be persuasive because receiving a message from a system and sending it to different systems is not new in the art and there are many examples for reception and transition of a message from one system to another system.

Applicant's argument in regard to **if and when the message is transmitted to a second system, the message is not sanitized** is not persuasive because Fahlman discloses the original message includes several sensitive terms (column 4, lines 20-21) and after removing the sensitive term and sanitization, the message is transmitted to an untrusted service (second system) which has lesser security level (see column 4, lines 64 and 65).

In regard to the claim amendment "**wherein said sensitive information is associated with said first security level"**, Fahlman teaches a method including different security levels. Message in step 205 of fig 2 includes sensitive information (first security level), which are identified (see column 4, lines 27) and sanitized (see column 4, lines 37-38) and then transmitted to an untrusted service (second security level) (column 3, lines 54-56 and column 4, lines 64-65). It is clear that untrusted service is not authorized to see the sensitive information and it has different security level. Therefore Fahlman teaches the amended limitation of the claim.

Regarding claims 13-20

Applicant argues that Fahlman does not teach **operating a sanitization tool for sanitizing a received message to generate first and second sanitized messages that differ based on respective first and second security levels**. Examiner respectfully disagrees because Fahlman clearly teaches a system with first level, second level or any level of security, in fact level

of the security could be adjusted to any desired level by replacing terms with the tokens (see column 4, lines 46-59).

Applicants argument in regard to Lindman does not teach **identifying first and second potential recipient having first and second security clearance** is not persuasive because in Lindman's security system before any communication takes place clearance at several security levels has to be identified, therefor Lindman teaches Identifying first and second security clearance (see column 4, lines 1-17).

Applicant argues that Lindman does not **teach identifying first and second sensitive information**. However, Lindham discloses a method of selecting unauthorized access mode based on verity of factors including "the degree of security deemed necessary to adequately protect data within central computer 14, and the **sensitivity of the data**" (see column 9, lines 28-32). Therefore it is clear that in Lindman can identify different (first and second) sensitive information because in Lindman's method in order to select unauthorized access mode different degrees of sensitivity of data must be identified.

In response to applicant's argument based upon the age of the references, contentions that the reference patents are old are not impressive absent a showing that the art tried and failed to solve the same problem notwithstanding its presumed knowledge of the references. See *In re Wright*, 569 F.2d 1124, 193 USPQ 332 (CCPA 1977).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

Regarding claims 21-29

Applicant's arguments regarding Fahlman **does not receive a message from a first system and transmitted to a second system after sanitization** and **If and when a message that Fahlman teaches is transmitted to a second system, the message is not sanitized** is not persuasive because of the same reason stated for claim 1-13. Applicant's argument regarding Fahlman's identification of sensitive information is not based on recipient is not persuasive because Fahlman teaches sanitizing or desanitizing the message based on the recipient of the message in another word the recipient has to be identified first and based on the security level of the recipient message is sanitized or desanitized. Therefor Fahlman's identification of sensitive information is based on recipient (see column 4,lines 49-59).

In response to applicant's argument that Fahlman teaches a method of **temporarily replacing sensitive terms with tokens for subsequent processing of a message that differs from the applicant's claim**, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claim 1-12 and 21-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Scott E. Fahlman et al. (US Patent NO.5,960,080).

Regarding Claim 1 and 27

Fahlman teaches a method (apparatus) for use in a multi-level secure system for sanitizing a message, said multilevel secure system including at least first and second security levels wherein first security level users are authorized to

receive sensitive information that second security level users are not authorized to receive, said method comprising the steps of: establishing a computer-based sanitization tool for sanitizing messages based on predefined sanitization, rules; (column 4, lines 17-67 and column5 lines 1-40) using said computer-based sanitization tool to receive a first message from a first external system, said first message including said sensitive information and additional information;(column 4 lines 20-22) first operating said computer-based sanitization tool to identify said sensitive information within said message (column 4 lines 28,29) and to sanitize said message relative to said sensitive information, thereby generating a first sanitized message different than said first message; (column 4 lines 42-43) and second operating said computer-based sanitization tool for transmission of said first sanitized message to a second external system, said second external system being associated with said second security level (column 4 lines 64-66).

Regarding Claim 2

Fahlman teaches a method, wherein said step of first operating comprises identifying said sensitive information based on said second security level and protecting said sensitive information such that said sensitive information is not useable by said second external system. (column 4 lines 17-65).

Regarding Claim 3

Fahlman teaches a method, wherein said step of first operating comprises accessing storage including multiple rule sets, using a parameter associated with said second security level to select a rule set, and applying said selected rule set with respect to the first message to generate said first sanitized message. column 3, lines 35-53).

Regarding Claim 4

Fahlman teaches a method, wherein step of second operating comprises identifying third external system associated with the third security level (column 6, lines 54-61 and fig 6 and associated text, discloses many options such as encryption. Examiner considers any option as another security level) operating said computer-based sanitization tool to generate a second sanitized message different than each of the said first message and said first sanitized message and operating said computer based sanitization tool for transmission of said second sanitized message to said third external system. (column 4, lines 20-67 and column 5, lines 1-34).

Regarding Claim 5, 24

Fahlman teaches a method, wherein said step of using comprises receiving a text only message. (column 4 lines 22-24).

Regarding Claim 6

Fahlman teaches a method, wherein said first message includes a graphics portion and said step of first operating comprises protecting sensitive

information within said graphics portion such that said sensitive information is not useable by said second external system. (column4 lines 22-26, 47-53).

Regarding Claim 7

Fahlman teaches a method, wherein said step of first operating comprises parsing said first message into a number of tokens and separately analyzing each token for said sensitive information. (column 4, lines 37-45).

Regarding Claim 8

Fahlman teaches a method, wherein said step of first operating comprises recursively parsing said first message to provide tokens of progressively smaller content until a desired parsing resolution is achieved and separately analyzing each token of said desired parsing resolution for said sensitive information. (column 4, lines 46-60).

Regarding claim 9

Fahlman teaches a method, wherein said step of second operating comprises identifying a first format associated with said second external system and converting said first sanitized message into said first format. (column4, lines 64-65).

Regarding claim 10 and 28

Fahlman teaches a method (apparatus), wherein said step of second operating comprises identifying a first format associated with said second external system, accessing storage including multiple specifications relating to multiple formats, retrieving from said storage first specification information for said first format and converting said first sanitized message into said first format using said first specification information. (column 4, lines 64,65 and column 3, lines 56-60).

Regarding claim 11

Fahlman teaches a method, further comprising the steps of generating a second sanitized message, the same or different than the first sanitized message, for transmission to a third external system, where said second external system is associated with a first format and said third external system is associated with a second format, first converting said, first sanitized message into said first format and second converting said second sanitized message into said second format.(column4 ,lines 20-65, column 5 lines 1-17).

Regarding claim 12

Fahlman teaches a method, further comprising the step of providing storage including first specification information for said first format and second specification information for said second format, where said step of first

converting comprise accessing said storage to obtain said first specification information and said step of second converting comprises accessing said storage to obtain said second specification information, wherein said storage can be used to reconfigure said sanitization tool for transmission in multiple formats without re-compiling.(column 2, lines 43-56).

Regarding claim 21

Fahlman substantially teaches a method for use in a multi-level secure system for sanitizing a message, said multi-level secure system including at least first and second security levels wherein first security level users are authorized to receive sensitive information that second security level users are not authorized to receive, said method comprising the steps of: establishing a computer-based sanitization tool for sanitizing messages based on predefined sanitization rules; (column 4, lines 17-64 and column 5, lines 1-40) first operating said computer-based sanitization tool for receiving a message and recursively parsing the message such that the message is parsed into tokens of a desired size;(column4, lines 38-53) second operating said computer-based sanitization tool for applying sanitization rules with respect to the parsed tokens to identify at least one dirty token relative to an identified recipient; and third operating said computer-based sanitization tool for sanitizing said message relative to said dirty token to generate a sanitized message for transmission to said identified

recipient. [(Examiner interprets dirty token as standard token)(column 4, lines 27-46)].

Regarding claim 22

Fahlman substantially teaches a method, wherein said step of second operating comprises identifying said at least one standard token based on a security level associated with said identified recipient and protecting said standard token such that said standard token is not useable by said identified recipient. (column 3, lines 27-67).

Regarding claim 23

Fahlman substantially teaches a method, wherein said step of second operating comprises accessing storage including multiple rule sets and using a parameter associated with said identified recipient to select said sanitization rules. (column 4, lines 37-67 and column 5, lines 1-20).

Regarding claim 25

Fahlman substantially teaches a method, wherein said message includes a graphics portion and said step of second operating comprises identifying said at least one standard token within said graphics portion. (column 4, lines 22-46).

Regarding claim 26

Fahlman substantially method, wherein said step of third operating comprises identifying a format associated with said identified recipient and

converting said sanitized message into said format.(column4, lines 64-65).

Regarding claim 29

Fahlman teaches an apparatus as, wherein said sanitization engine is operative for identifying a potential recipient of said message and obtaining said at least one sanitization rule based on said intended recipient.(column 3, lines 27-67 and column 7, lines 7-10).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 13-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott E. Fahlman et al. (US Patent NO.5, 960,080). in view of Richard S. Lindman et al.(US Patent NO.4,882,752).

Regarding Claim 13, 14, 15

Fahlman teaches a method for use in a multi-level secure system for sanitizing a message, said multi-level secure system including at least first and second security levels wherein first security level users are authorized to receive sensitive information that second security level users are not authorized to receive, said method comprising the steps of: establishing a computer-based sanitization tool for sanitizing messages based on predefined sanitization rules;(column 4, lines 17-64, column 5, lines 1-40). first using said computer-based sanitization tool for receiving a message for potential distribution;(column 4, lines 20-22). Third operating aid computer-based sanitization tool for sanitizing said received message to generate first sanitized message for transmission to said first potential recipient (column 4, lines 20-46) and fourth operating said computer-based sanitation tool for sanitizing said received message to generate a second sanitized message, different than the first sanitized message, for transmission to said second potential recipient. (column 4, lines 20-67 and column5, lines 1-28).protecting first and second sensitive information such that first sensitive information is not useable by first potential recipient and second sensitive information is not usable by second potential recipient.(column 4, lines 46-53). Fahlman does not teach second operating said computer-based sanitization tool for identifying at least first and second potential recipients having first and second security clearances and identifying first and second sensitive information based on first and second security clearances andaccessing storage

including multiple rule sets, using parameters associated with first and second security clearances to select a first rule set, second rule set. However Lindman discloses a method of different levels of security clearances (column 8, lines 65-68, column 9, lines 1-8 and column 10, lines 16-49) and identifying first and second sensitive information based on first and second security clearances. (column 8 lines 65-68, column9, lines 1-8 and column 10, lines 16-49). Accessing storage including multiple rule sets and using parameters associated with the first and second security clearances to select the first and second rule sets. (column 8, lines65-68,column 9 lines 1and column 10, lines 16-24). Therefor it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Fahlman to include the first and second security clearances for at least first and second potential recipient. identifying first and second sensitive information based on first and second security clearances and accessing storage including multiple rule sets, using parameters associated with first and second security clearances to select a first rule set and second rule set This modifications could have been obvious because person having ordinary skill in the art would have been motivated to do so in order to provide several security levels to prevent access by unauthorized recipient and spread of private information outside of the trusted environment.

Regarding Claim 16

Fahlman teaches a method, wherein said step of first using

comprises receiving a text only message. (column 4, lines 22-24).

Regarding claim 17

Fahlman teaches a method, wherein said message includes a graphics portion and said step of third operating comprises protecting sensitive information within said graphics portion such that said sensitive information is not useable by said first recipient. (column 4, lines 22-26,47-53).

Regarding Claim 18

Fahlman teaches a method, wherein said step of third operating comprise parsing said message into a number of tokens and separately analyzing each token for sensitive information. (column 4, lines 37-45).

Regarding claim 19

Fahlman teaches a method, wherein said step of third operating comprises identifying a first format associated with said first potential recipient and converting said first sanitized message into said first format, and said step of fourth operating comprises identifying a second format associated with said second potential recipient and converting said second sanitized message into said second format. (column 3, lines 56-60, column 4, lines 64-65 and column 5, lines 1-17).

Regarding Claim 20

Fahlman teaches a method, further comprising the step of providing storage including first specification information for said first format and second

specification information for said second format, where said step of third operating comprises accessing said storage to obtain said first specification information and said step of fourth operating comprises accessing said storage to obtain said second specification information, wherein said storage can be used to reconfigure said sanitization tool for transmission in multiple formats without re-compiling.(column 2, lines 43-56).

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

Ali Abyaneh A.A
Patent Examiner
Art Unit 2137
10/15/05